**Testimony of Michael Altschul, Senior Vice President and General Counsel,
CTIA – The Wireless Association®
before the
House Energy and Commerce
Subcommittee on Communications, Technology, and the Internet, and
Subcommittee on Commerce, Trade, and Consumer Protection**

February 24, 2010

On behalf of CTIA – The Wireless Association® ("CTIA"), I want to thank Chairman Boucher and Chairman Rush, ranking members Stearns and Radanovich, and members of the two subcommittees for the opportunity to appear at today's hearing to share the wireless industry's views on the proper regulatory framework for location-based services.

My name is Mike Altschul, and I have served as CTIA's General Counsel since 1990. In my capacity at CTIA, I have been involved in the development of CTIA's Best Practices and Guidelines for Location-Based Services ("Guidelines"). I have represented CTIA before the Federal Trade Commission and the FTC's activities related to privacy and location-based services, the most recent of which was the January 28, 2010 "Exploring Privacy" roundtable held at the University of California, Berkeley, School of Law. Additionally, I have been involved with CTIA's advocacy on these issues before the Federal Communications Commission.

CTIA has been at the forefront of location privacy while balancing the need for legitimate access to a customer's location information in emergencies and for law enforcement purposes from the inception -- beginning fifteen years ago when CTIA and Public Safety proposed a "Consensus Solution" to the Federal Communications Commission's wireless E-911 rulemaking proceeding. I am proud that CTIA has been a leader in regard to location privacy ever since. In the late 1990s, we supported *The Wireless Communications and Public Safety Act of 1999* (Public Law 106-81, 113 Stat. 1286-1290), which addressed some of the issues that arose from the FCC's E-911 rulemaking, including a provision that specifically authorized carriers to

provide call location information concerning a user of a commercial mobile service to: (1) emergency dispatchers and emergency service personnel in order to respond to the user's call; (2) the user's legal guardian or family member in an emergency situation that involves the risk of death or serious physical harm; or (3) providers of information or data base management services solely for assisting in the delivery of emergency services. Significantly, *The Wireless Communications and Public Safety Act* also amended Section 222 of the Communications Act to require "the express prior authorization of the customer" for the disclosure of the wireless customer's location information for any other purpose.

In 2000, CTIA petitioned the FCC to adopt a set of Fair Location Information Practices for wireless location-based services. CTIA's proposal was modeled on the familiar Fair Information Practice Principles. Although the FCC declined to adopt CTIA's proposal, the fundamental principles of customer "notice" and "consent" have been widely adopted and continue to provide the basis for the wireless industry's approach to location-based services.

Two years ago, as location-based services began to be developed and deployed for applications other than E-911, CTIA worked with its members and other interested parties to develop a set of industry "Best Practices and Guidelines" to promote and protect the privacy of wireless customers' location information. The 2008 Guidelines directed the entities that provide location based services to inform users about how their location information will be used, disclosed, or protected so that a user can make an informed decision about whether or not to use a particular location-based service or authorize disclosure of his or her location. Additionally, once a user has opted to use a location-based service, or authorized disclosure of his or her location, the 2008 Guidelines contemplate that the user should have choices as to when or whether location information would be disclosed to third parties, as well as providing that the user should have the ability to revoke such authorization at any time.

In crafting the 2008 Guidelines, we recognized, consistent with Section 222 of the Communications Act, and the FCC's rules governing Customer Proprietary Network Information ("CPNI"), that user privacy must be balanced with legitimate law enforcement and emergency or other needs. Accordingly, the guidelines did not apply to location information used or disclosed:

- as authorized or required by applicable law (e.g., to respond to emergencies, E911, or legal process);
- to protect the rights and property of LBS providers, users or other providers of location information;
- for testing or maintenance in the operation of any network or LBS; or
- in the form of aggregate or anonymous data.

Today, we are in the process of revising the 2008 Guidelines. Why are we revising the Guidelines so soon? Up until recently, there was a widely held assumption that location-based services would involve a wireless carrier having access to a user's location information and then using or sharing that information to provide a location-based service. That is what Congress contemplated when it enacted amendments to Section 222 of the Communications Act as part of the *Wireless Communications and Public Safety Enhancement Act of 1999*, and that is what we envisioned just two years ago as we worked with our members to craft what became the 2008 Guidelines.

As is often the case, things turned out a bit differently than had been envisioned, as the last two years have brought profound change to the wireless industry. The rapid evolution toward open platforms, the overwhelming consumer adoption of smart-phones, and the increased prevalence of GPS-enabled location-based service applications that can be downloaded to a handset and enabled without any involvement or knowledge by a wireless carrier[1] combined in a way that suggested that a carrier-centric approach to location-based service guidelines is no longer

[1] An overview of non-carrier provided location based services can be found at http://www.ftc.gov/os/comments/privacyroundtable/544506-00088.pdf.

sufficient or even desirable. These factors led us to reevaluate the 2008 Guidelines, and as we complete work on the 2010 Guidelines, we envision that they will ensure that there is always one clearly identified location-based services provider with the obligation to inform the user as to how location information will be used and disclosed and to obtain the user's consent before initiating the service. Under the revised Guidelines, the user will always know who is responsible for the careful handling of his or her location information. We will be working with our members and other interested parties to push for broad acceptance of the Guidelines.
While the scope of the new Guidelines is different, the focus is not. The new Guidelines will build on the foundation we laid ten years ago by continuing to put a premium on user notice and consent.

With respect to notice, we envision that location-based service providers ought to ensure that potential users are informed about how their location information will be used, disclosed and protected so that they can make informed decisions whether or not to use a particular service, giving the user ultimate control over their location information.

The Guidelines envision that location-based service providers will use written, electronic or oral notice that will ensure that users have an opportunity to be fully informed of the providers' information practices. Notice must be provided in plain, easily understood language, it must not be misleading, and if combined with other terms or conditions, the portion pertaining to the location-based service must be conspicuous.

If, after having obtained consent, a provider of location-based services wants to use location information for a new or materially different purpose not disclosed in the original notice, the provider must inform the user with further notice and obtain the user's consent to the new or other use.

The Guidelines also dictate that location-based service providers must inform users how long any location information will be retained, if at all. As a general matter, providers should retain user location information only as long as business needs require, after which such information should be destroyed or rendered unreadable.

Additionally, the Guidelines also direct location-based service providers to periodically remind users when their location information may be shared with others and of the users' location privacy options. The specific terminology, timing and frequency of such notice depends on the nature of the particular service. For example, one would expect more reminders when the service involves frequent sharing of location information with third parties and fewer reminders, if any, when the service involves a one-time, user-initiated concierge service call (e.g., a call requesting a nearby service).

Another significant change from the 2008 Guidelines is the clear requirement that every user be informed whenever a location-based service is installed and used on their device. In some circumstances, account holders (as opposed to users) may control the installation and operation of location-based services (e.g., business account holder utilizing a location service for fleet management or a parental account holder providing phones for use by a child or member of a "family plan"). In addition to providing notice to the account holder, location-based service providers must ensure that notice is provided to each user that location information is being used by or disclosed to the account holder or others. This now clearly stated requirement will reduce the risk of surreptitious or unauthorized tracking. While we do not believe this is required by Section 222 – which addresses the rights of the "customer" and not the rights of the "user," we believe it is the right approach to promoting and protecting user privacy.

In addition to providing significant guidance regarding the type of notice that users should expect, the Guidelines will continue to speak to the issue of consent.

CTIA's Guidelines contemplate that location-based service providers will obtain user consent to the use or disclosure of location information ***before*** initiating a location-based service. The form of consent may vary with the type of service or other circumstances, but location-based service providers bear the burden of establishing that consent to the use or disclosure of location information has been obtained before initiating service.

The Guidelines require that consent be informed and based on a notice consistent with the notice requirements set forth by the Guidelines. Consent may be implicit, such as when users request a service that obviously relies on the location of their device. Notice may be contained in the terms and conditions of service for a location-based service to which users subscribe. Users may manifest consent to those terms and conditions electronically by clicking "I accept"; verbally by authorizing the disclosure to a customer service representative; through an IVR system or any other system reasonably calculated to confirm consent. The Guidelines expressly reject pre-checked boxes that cause a user to be automatically opted-in to location information disclosure or choice mechanisms that are buried within a lengthy privacy policy or a uniform licensing agreement. Such an approach would be insufficient to express user consent under the CTIA Guidelines.

Users should have confidence when obtaining a location-based service from those location-based service providers that have adopted the Guidelines that their location information will be protected and used or disclosed only as described in provider notices. By receiving notice and providing consent consistent with these practices, users will maintain control over their location information.

The Guidelines encourage providers of location-based services to develop and deploy new technology to empower users to exercise control over their location information and to find ways to deliver effective notice and obtain consent regardless of the

device or technology used or business model employed. CTIA supports the ongoing and continuous education of users so they may make informed choices.

We believe the Guidelines offer a meaningful framework for the protection of user privacy. Further, we urge policymakers to recognize that the industry's willingness to develop best practices, and to revise those guidelines as circumstances warrant, represents the best way to balance the need to promote and protect user privacy while also facilitating the deployment of new and innovative products and services.

A call for legislative restraint does not mean that there is no role for Congress while the industry evolves. Congress already has made clear that "the express prior authorization of the customer" is the prerequisite for the disclosure of a wireless customer's location information. While Section 222 on its terms applies only to "telecommunications carriers," its requirements have been observed by all providers of wireless location-based services. As these services continue to evolve and develop in both predictable and unpredictable ways, Congress has an important oversight role in insuring that all providers of location-based services continue to deliver effective notice and obtain consent regardless of the device or technology used, and regardless of the provider's business model, so that wireless users can continue to exercise control over the use or disclosure of their location information.

One area in which specific guidance from Congress may be appropriate is the clarification of the terms under which location information may be released to law enforcement. Just this month, the U.S. Court of Appeals for the Third Circuit heard oral argument on the issue of what legal standard should apply when law enforcement seeks to gain access to a wireless user's location information records, or seeks to track individuals prospectively. Many federal magistrates have determined that law enforcement must obtain a warrant based on probable cause to prospectively track a device. Other magistrates have authorized tracking on a lower standard. Most courts have allowed access to stored location records based on a court order and

demonstrated need, but in the Third Circuit, the Department of Justice and privacy advocates argued whether access to these historical location records should meet a probable cause standard. Service providers need clarity so as to not be caught in the middle of these disputes regarding the appropriate legal standard.

Finally, we urge Congress to recognize the interstate nature of location-based services, and the mobile nature of wireless users, and to take care in whatever framework may be adopted to preempt state regulation of these service offerings. A uniform, national approach to these issues presents the best way of protecting user privacy and educating and informing wireless customers while fostering innovation, investment, and the introduction of new location based services by wireless carriers, device manufacturers, operating systems developers, and applications creators.

On behalf of CTIA, thank you again for the opportunity to share our views with the subcommittees. We look forward to working with you as you continue your efforts.

# # #